Novagraaf
A NovumIP Company

Protection de marques en ligne

Guide pratique

A propos de Novagraaf

Depuis plus de 130 ans, Novagraaf aide les marques emblématiques et les organisations innovantes du monde entier à se doter d'un avantage concurrentiel. Novagraaf, leader Européen de Conseils en Propriété Intellectuelle, est spécialisé dans la protection et la gestion globale des droits de Propriété Intellectuelle, notamment les marques, les brevets, les dessins et modèles, les noms de domaine et les droits d'auteur. Basé aux Pays-Bas, Novagraaf dispose de 17 bureaux dans le monde et d'un puissant réseau de plus de 330 spécialistes.

Pour en savoir plus, consultez le site **www.novagraaf.com**

Introduction

Vos marques sont surexposées à travers les marketplace, les sites internet, les réseaux sociaux, les applications, les noms de domaine et tout autres moyens de communication ou de commercialisation digitales. Toutefois, même si l'offre en ligne ne manque jamais, la fiabilité et la qualité ne sont pas toujours au rendez-vous.
En effet, vos marques sont trop souvent la première cible des fraudeurs qui cherchent à détourner le trafic en ligne ou à profiter de consommateurs peu méfiants. D'ailleurs, l'épidémie de la COVID-19 n'aura pas freiné les contrefacteurs et leur (in) délicatesse pour déposer des marques en France ou dans l'Union Européenne autour de termes tels que COVID-19 ou Coronavirus. Nous comptons de très nombreuses atteintes aux droits sur internet pendant la période de pandémie, et les conséquences sur vos marques sont graves.
Certes il existe des procédures établies pour agir contre ces menaces en ligne, mais ce serait une erreur de penser que les propriétaires de marques gagnent toujours la bataille de la protection et la défense de leurs droits sur le web. En fait, la nécessité de préserver la réputation de votre marque, de protéger votre entreprise et vos clients contre les contrefacteurs, et de renforcer votre présence numérique contre les squatters de noms de domaine devrait déjà se positionner comme étant la priorité dans votre stratégie de Propriété Intellectuelle.

Dans un monde où la complexité et la connectivité continue sont devenues la nouvelle norme, les anciennes approches de la protection des marques en ligne ne sont plus adaptées. Mettre en œuvre des stratégies efficaces de protection des marques en ligne sans y investir trop de temps et de précieuses ressources internes, est devenue l'un des principaux défis auxquels sont confrontées les entreprises aujourd'hui.

C'est pourquoi Novagraaf s'est mis au défi de trouver une solution adaptée aux différents types d'entreprises, en combinant son expertise juridique à ses atouts en matière de technologie.
Nous sommes fiers de vous annoncer que notre service de protection en ligne dispose désormais d'un outil entièrement intégré et automatisé, vous permettant d'accéder instantanément au suivi de la surveillance de votre marque en ligne, aux recommandations de nos experts face aux menaces identifiées, et aux impacts des actions mises en oeuvre.
Nous espérons que ce nouvel outil et les conseils que nous partageons dans ce Livre blanc vous aideront à vous sensibiliser et armer votre marque et vos entreprises aux défis auxquels nous sommes confrontés.

Découvrez dans ce Livre blanc, les conséquences des infractions en ligne portées sur les marques, et nos astuces et solutions de surveillance et de protection des marques en ligne vous permettant d'agir rapidement et de manière proportionnée, en impactant au minimum vos équipes.
Pour finir, Novagraaf vous dévoilera les clés pour doter votre marque d'un triple atout : innovant, sécurisé et valorisé afin d'anticiper sur l'environnement numérique complexe de demain.

Olivier Boland
Président Directeur Général
Novagraaf France :
tm.fr@novagraaf.com

Faites analyser gratuitement votre marque en ligne !
Les lecteurs de ce Livre blanc sont invités à s'inscrire pour recevoir gratuitement un apercu de l'une de leurs marques en ligne. L'analyse permettra d'identifier les menaces qui pèsent sur cette marque en ligne et de recevoir des recommandations juridiques à apporter.
Pour en savoir plus : **novagraaf.com/fr/brand-protection**.

L'APRÈS COVID-19 : POUR LES MARQUES, IL S'AGIT AVANT TOUT D'UNE QUESTION DE CONFIANCE ET DE FIABILITÉ

La panique liée à la pandémie a entraîné une forte augmentation de la demande de produits, de services et d'informations en ligne

Ces dernières années, le commerce en ligne a permis à un nombre croissant de personnes d'accéder à des produits et services qui leur étaient jusqu'alors soit inconnus, soit inaccessibles. En outre, il a également apporté un niveau de commodité que les achats traditionnels ne peuvent pas offrir – à savoir, il n'est maintenant plus nécessaire de se rendre dans un magasin pour obtenir les biens désirés et il est possible d'en obtenir la livraison quasi instantanée. L'accès à l'information a également fait un bond en avant extraordinaire : les sites web et, plus récemment, les plateformes de médias sociaux, facilitent et accélèrent maintenant la communication de faits et d'opinions à l'échelle mondiale.

La crise du Covid-19 a poussé nombre d'entre nous à repenser notre présence numérique et a créé en peu de temps une hausse importante et sans précédent de la demande de produits, de services et d'informations en ligne. Elle a effectivement aussi eu pour effet de surcharger cet environnement de manière significative. Alors que les gens sont interdits de place publique et mis en confinement, il n'en demeure pas moins qu'ils ont encore des besoins à satisfaire, et dans de nombreux cas, seul Internet peut y pourvoir.

Compte tenu de la nature sanitaire de la crise et des mesures de confinement qui ont été mises en place dans de nombreux pays, certaines industries ont ainsi connu une forte augmentation dans la demande de leurs produits et, dans de nombreux cas, se sont également heurtées à des problèmes d'approvisionnement.

Ceci peut être observé sur trois catégories. Premièrement, la demande de produits sanitaires et de santé liés à la pandémie, tels que les désinfectants pour les mains, les masques et les kits de diagnostic, a grimpé en flèche - ce qui n'est en soi pas surprenant. La demande de livraison de nourriture via une commande en ligne, due au confinement et à la peur d'une contamination physique dans les supermarchés, ainsi que de produits et services de loisirs, tels que livres, jeux ou encore services de streaming, a également augmenté de manière significative. Enfin, l'éloignement social, l'isolement forcé et le travail à distance ont créé un besoin profond et fondamental d'informations en ligne et la production de formes alternatives d'interaction sociale. On a ainsi assisté à la multiplication des sources d'information, à une forte augmentation de la consommation de médias sociaux et à la montée en puissance de services tels que Zoom et Microsoft Teams.

L'information : un bien précieux où la fiabilité de la marque source est cruciale

Dans ce contexte de pandémie, l'un des biens les plus précieux s'est avéré être l'information. Et l'offre n'a pas manqué, bien au contraire. Toutefois, la qualité et la fiabilité de l'information ont été plus que variables.

La fiabilité de l'information est généralement garantie du fait d'une marque source reconnaissable et faisant autorité. Par exemple, les « Centers for Disease Control and Prevention » (CDC) aux États-Unis, le « National Health Service » (NHS) au Royaume-Uni et l'Organisation Mondiale de la Santé (OMS) sont largement considérés comme étant des sources fiables sur lesquelles fonder des actions de santé publique, que ce soit au niveau communautaire ou individuel. C'est pourquoi ces institutions ont été des cibles de choix des profiteurs ainsi que des fraudeurs imitent les noms et les logos de ces sources fiables, afin diffuser leurs propres informations – ou désinformations dans ce cas. Étant donné que ces logos fonctionnent comme un label de confiance, les gens tendent en effet à consommer ces informations avec confiance.

En réponse à ce détournement et à la dévaluation de leurs marques, que l'OMS a également judicieusement qualifié d' « infodémie », ces institutions ont rapidement du prendre des mesures. CNN Business rapporte notamment que l'OMS a forgé une alliance avec les grandes entreprises technologiques, dont Facebook et Google, afin de limiter la propagation de désinformations potentiellement dangereuses. Le World Trademark Review (WTR) rapporte que le NHS a conclu un accord similaire avec Google. Dans une déclaration publiée sur Facebook le 4 mars 2020, Mark Zuckerberg a affirmé que « Compte tenu de l'évolution de la situation, nous travaillons avec les ministères nationaux de la santé et des organisations comme l'OMS, les CDC et l'UNICEF pour les aider à diffuser des informations précises et opportunes sur le coronavirus. » En outre, dans le sillage de ces actions, les

principales sociétés de médias sociaux ont publié une déclaration commune de l'industrie exprimant leur détermination à lutter contre la fraude et la désinformation sur le virus et à promouvoir sur leurs plateformes un contenu de qualité faisant autorité et provenant de sources fiables.

Escroqueries et contrefaçons ou comment tirer facilement profit de la pandémie

L' « infodémie » et ses conséquences pour la santé publique n'est pas le seul problème que le Covid-19 a catalysé ces derniers mois sur Internet. L'augmentation de la demande de produits sanitaires et médicaux, tels que les désinfectants pour les mains, les masques et les gants de protection, ainsi que l'incapacité des détaillants habituels à fournir ces produits ont créé des conditions idéales pour que des fournisseurs tiers puissent combler le vide ainsi crée. L'un des principaux problèmes résultant de l'émergence de ces vendeurs non conventionnels a été la flambée des prix.

Un cas particulièrement illustratif est celui des frères Colvin qui, au début de la maladie aux États-Unis, ont pris la route du Tennessee jusqu'au Kentucky pour acheter autant de désinfectant pour les mains et de lingettes désinfectantes qu'ils ont pu trouver. Leur but était évidemment de faire un profit singulier en vendant ces produits – ils avaient bien anticipé la hausse des demandes – à une marge bénéficiaire aussi élevée que possible sur Amazon. Malgré une réelle demande, leur initiative s'est toutefois avérée de courte durée et ils se sont retrouvés avec pas moins de 17'700 bouteilles de désinfectant pour les mains, comme le rapporte le New York Times. En effet, les critiques croissantes des régulateurs et des clients ont incité Amazon et d'autres plateformes similaires à sévir contre les prix abusifs sur leurs places de marchés. Il est à noter que ces mesures étaient en définitive destinées à protéger non seulement les clients, mais aussi la réputation d'Amazon en tant que plateforme fiable et de confiance.

Un autre problème qui s'est posé avec l'arrivée sur le marché de vendeurs « tiers » a été celui de la qualité des produits. L'achat de produits en ligne implique, d'une certaine manière, un acte de foi : après tout, vous ne pouvez pas vérifier la qualité d'un produit ni la fiabilité de votre vendeur, comme vous le feriez dans un centre commercial, au supermarché ou dans le quartier commerçant de votre ville. Le moment de vérité tombe lorsque le colis arrive par la poste. La contrefaçon en ligne ne date pas d'hier et remonte aux premiers jours du commerce électronique. Ceci dit, l'ampleur du problème a pris des proportions bien plus importantes à cause du Covid-19, avec un marché chaotique où les acheteurs se précipitent pour acquérir les produits disponibles le plus rapidement possible et où les vendeurs cherchent à tirer profit d'une demande accrue. Les médias ont ainsi fait état de nombreux cas d'équipements défectueux, de produits périmés, de contrefaçons et de prétendus remèdes miracles. The Guardian rapporte notamment que la FDA a adressé une lettre d'avertissement à Jim Bakker, un éminent télévangéliste, qui avait autorisé l'un de ses invités à promouvoir et à vendre pendant son show de l'argent colloïdal comme remède contre le Covid-19, cette substance étant considérée comme ni sûre ni efficace par la « Food and Drug Administration » (FDA) et potentiellement dangereuse par les « National Institutes of Health » (NIH).

De la recherche de profit à la fraude pure

Nous avons observé plus haut que la question clé est celle de la fiabilité, dans un cas de l'information, dans l'autre de produits. Cette fiabilité se communique en invoquant des noms reconnus, source de cachet et d'autorité, ou signalant leur actualité et utilité par des mots-clés bien définis. Étant donné que les noms de domaine fonctionnent comme des enseignes de magasin en ligne, ils sont souvent la première cible de fraudeurs qui cherchent à diriger le trafic en ligne vers leurs domaines, ou simplement de profiteurs cherchant de l'argent facile et rapide. Il était donc plus ou moins inévitable que les noms de domaine ne soient pas épargnés pendant le Covid-19.

Les préjudices que peuvent causer les noms de domaine sont multiples et correspondent à ceux que l'on retrouve sur les plateformes de médias sociaux et les sites marchands. Mais outre la désinformation et la vente de contrefaçons, il est intéressant de noter que durant le Covid-19, les noms de domaine ont également été abondamment utilisés à des fins de spéculation. En effet, les noms de domaine contenant des termes susceptibles d'attirer un grand nombre de personnes peuvent être particulièrement précieux, ce qui a conduit à des activités spéculatives dans lesquelles des noms de domaine ont été achetés dans la perspective de les revendre à fort profit. Les noms de domaine contenant des termes tels que coronavirus, covid, vaccin, diagnostic et tests ont aisi proliféré comme des champignons après la pluie. Cela a conduit certains bureaux d'enregistrement, comme Namecheap, à renforcer le contrôle de certains mots clés et à supprimer de leur outil de recherche des mots tels que "coronavirus", "covid" et "vaccin". En ce qui concerne les ccTLDs, EURid et Nominet ont, pour leur part, mis en place des procédures garantissant que les espaces de nommage .eu et .uk soient aussi libres que possible des noms de domaine enregistrés à des fins d'exploitation ou de malveillance.

Plus dangereux encore, cependant, est l'utilisation d'un nom de domaine imitant des sources officielles largement reconnues ou faisant autorité pour signaler leur fiabilité en matière d'information. Les organismes officiels ont ainsi reconnu, pendant la pandémie, le risque élevé que leurs noms ne soient utilisés pour de l'hameçonnage et d'autres formes de cyberattaques. La montée soudaine des outils de communication en ligne pour répondre aux impératifs d'isolement social a effectivement à son tour inspiré une vague de sites web de hameçonnage qui cherchaient à diriger le trafic

vers eux en imitant les grandes marques et les plateformes légitimes.

Conclusion

La nécessité de préserver la réputation de votre marque, de protéger votre entreprise et vos clients de l'exploitation et des contrefacteurs et de renforcer votre présence numérique contre les cybersquatters devrait déjà figurer en bonne place dans votre stratégie de propriété intellectuelle pour 2020. Toutefois, l'épidémie de COVID-19 aura renforcé cette priorité – et pour cause.

Pour maintenir la confiance dans votre marque, il faut faire preuve de prévoyance et élaborer une stratégie de protection des marques en ligne qui protégera votre marque et lui fournira les conditions nécessaires pour s'épanouir dans le monde numérique, aujourd'hui et demain. Ainsi, lorsque vos clients vous contacteront en ligne, ils pourront être rassurés en sachant que c'est vraiment vous qu'ils trouveront de l'autre côté.

Anca Draganescu-Pinawin
Conseil en Propriété Industrielle – Marques, Dessins et Modèles, dirige le service de protection des marques en ligne - Novagraaf, Suisse.
Pour la contacter : brandprotection@novagraaf.com.

Les atteintes aux droits sur internet en période de pandémie … et après ?

En toute situation de crise, se voient proliférer des profiteurs aux intentions malveillantes, et la période de pandémie que nous vivons actuellement ne fait malheureusement pas exception. En effet, Internet devient le terrain de jeux de cybercriminels et autres contrefacteurs, et leur imagination ne cesse de se développer pour trouver des moyens toujours plus originaux ou novateurs afin de tirer profit d'une situation déjà complexe, au détriment des droits ou de l'image d'entités privées ou publiques.

Noms de domaine et sites internet revêtent aujourd'hui des enjeux économiques stratégiques pour une personne physique ou morale souhaitant étendre ou accroître une activité, et de ce fait, sont bien souvent la cible d'agissements parasitaires.

Les atteintes portées aux marques sur les noms de domaine, sites internet, réseaux sociaux, applications et autres moyens de communication ou de commercialisation digitales se sont multipliées ces derniers temps et il est fort à craindre que cette tendance ne va s'amplifier du fait du développement exceptionnel et exponentiel du e-commerce.

Cette multiplication de sites de commerce en ligne, via notamment les places de marché, entraîne inéluctablement un accroissement des atteintes portées aux droits des tiers.

Il est donc impératif pour tout à chacun de se doter aujourd'hui de moyens efficaces afin de pouvoir réagir demain contre ces fraudes et de se munir de solutions afin permettant de les déceler en amont.

Les différentes atteintes sur Internet en période de crise

Cybersquatting, hameçonnage, spam, usurpation ou encore contrefaçon font parties des nombreuses atteintes à l'encontre desquelles entreprises et particuliers doivent faire face.

Ainsi, dès le début de la crise sanitaire, l'Organisation Mondiale de la Santé a été visée par une attaque en faisant l'objet de « phishing » (technique faisant croire à une victime qu'elle s'adresse à un tiers de confiance et visant à obtenir des renseignements personnels aux fins d'usurpation d'identité).

S'en est suivie, une vague considérable d'achats de noms de domaine reprenant des mots clés liés au virus tels que « covid », « covid-19 » ou « coronavirus » dans un premier temps, puis des réservations composées de « chloroquine », « déconfinement », « test » ou encore « masques » dans un deuxième temps. Ainsi, il a pu être recensé plus de 6000 réservations de noms de domaine par jour, qui seraient potentiellement litigieuses ou avec une intention d'exploitation malveillante en lien avec la situation sanitaire. DomainTools a établi et publié une liste de noms de domaine avec pour chacun un risque de dangerosité.

Ces noms de domaines sont alors utilisés soit pour la revente (des réservataires souhaitant tirer profit de la crise en mettant aux enchères des noms de domaine à des prix allant jusqu'à plusieurs milliers d'euros), soit pour des sites d'appel aux dons au profit d'associations fictives, soit pour vendre un produit contrefaisant, soit encore pour des sites de vente en ligne de produits sans lien avec le virus.

A titre d'exemples, des noms de domaine tels que « covid19.com », qui propose plusieurs liens dont l'un sur le site officiel de l'OMS et les autres sur des sites d'appel aux dons, ou « stopcovid.fr » n'ont pas été réservés ni par l'OMS ni par le gouvernement mais par des particuliers.

Ou encore des noms de domaine tels que « tests-coronavirus.fr ». « corona-vaccination.fr », « masquescovid-19 », « protectcoronavirus.fr » sont encore à vendre dans l'espoir de trouver acquéreur à plusieurs centaines d'euros. Si l'engouement pour ces noms de domaine et les spéculations y afférentes vont vraisemblablement vite retomber dans la mesure où la dénomination « COVID » n'est pas une marque, et donc libre de droit, des situations plus critiques associent des noms de domaine litigieux à une marque pouvant être particulièrement problématiques pour les titulaires de droit.

C'est ainsi que, après le dépôt d'une plainte administrative, le Centre d'arbitrage et de médiation de l'OMPI a ordonné le 5 mai dernier le transfert du nom de domaine « coronagileadsciences.com » au profit de la société titulaire des droits de marque, Gilead Sciences, Inc. (Litige n°D2020-0776).

Plusieurs registres en charge de l'enregistrement de noms de domaine de premier niveau national (ccTld) ont pris certaines mesures afin de pouvoir réagir à l'encontre de cette vague exceptionnelle d'atteintes.

Ainsi, le registre chargé de la gestion du .eu (EURID) a mis en place un système dénommé APEWS (« Abuse Prevention and Early Warning System »), permettant de détecter qu'un nom de domaine serait source d'abus potentiels. Dans ce cas, le système retarde sa délégation dans la zone .eu et sera sous un statut spécifique de « server hold », jusqu'à la vérification complète de cette réservation par les services de l'EURID qui procédera ensuite à sa suspension dans les cas les plus suspects. Le registre britannique a mis en place, quant à lui, un système de suspension de plusieurs centaines de noms de domaine frauduleux.

Sans attendre que les registres tentent de lutter contre ces atteintes, et ne pouvant toutes les enrayer, c'est au titulaire de droits à prendre les mesures nécessaires en amont afin de :

- mettre en place des gardes fou permettant de limiter les risques d'atteinte ;
- détecter et évaluer les menaces et/ou les atteintes sur l'ensemble des supports web : applications mobiles, réseaux sociaux, places de marché, site internet et noms de domaine ;
- réagir rapidement à l'encontre de l'usage frauduleux de la marque et stratégiquement pour faire cesser le préjudice.

Afin de pouvoir mettre en place les moyens adéquats pour se prémunir de ces atteintes, nous rappelons l'intérêt pour les entreprises de mener des audits sur leur propre exploitation et particulièrement sur leur portefeuille de noms de domaine afin de pouvoir identifier :

- les noms de domaine stratégiques : site web, site e-commerce, messagerie, sous-domaine, VPN…
- les noms de domaine défensifs dont l'intérêt est moindre mais qui seraient susceptibles d'être préjudiciables en cas de réservation par un tiers ;
- les noms de domaine périphériques n'ayant pas d'intérêt (récupération suite à une plainte, ancienne campagne marketing…) et pouvant faire l'objet d'économie.

Ce classement permet ensuite de pouvoir identifier et prioriser les réactions en fonction de la pertinence de chacun des noms de domaine.

En effet, plusieurs stratégies peuvent être mises en place afin de sécuriser vos droits, de limiter le caractère préjudiciable d'un acte malveillant et d'anticiper ces potentielles atteintes :

- La mise en place de mesures techniques de sécurisation des noms de domaines et sites internet appartenant au titulaire des droits : cela permet de limiter les risques d'attaque, ou du moins de les rendre plus difficiles, contre le site internet de l'entreprise, susceptibles d'entrainer un détournement administratif et technique du trafic. Il s'agit du système dit de « Registry Lock » permettant de bloquer toute usurpation par un processusd'authentification auprès du registre. L'intérêt n'est pas de mettre en place ces sécurisations sur l'intégralité des noms de domaine mais de cibler aux noms de domaine les plus stratégiques.

- Une demande de levée d'anonymat ou de vérification des données whois afin d'exercer un contrôle sur le titulaire du nom de domaine, en cas de réservation frauduleuse de noms de domaine sous couvert d'anonymat.

- L'établissement d'une stratégie de réaction en fonction de l'atteinte portée : le choix et la manière de réagir doivent être proportionnés au préjudice subi ou au risque de préjudice à venir. En effet, plusieurs réponses sont susceptibles d'être portées à des destinataires différents selon la responsabilité de chacun (Provider, bureau d'enregistrement, hébergeur…).

- Concernant les réseaux sociaux, la plupart a mis en place des procédures de plainte en ligne (Facebook, Twitter, Instagram…). En effet, ces sites sont le plus souvent considérés comme des hébergeurs leur octroyant une responsabilité allégée mais ayant l'obligation de devoir prendre les mesures nécessaires à la cessation d'une atteinte dès qu'ils en sont informés.

- Des procédures extra-judiciaires : de nombreuses procédures administratives de règlement des litiges sont aujourd'hui ouvertes aux titulaires de droit, et elles ont l'avantage d'être rapides, économiques et efficaces (récupération ou abandon du compte ou nom de domaine litigieux). En fonction de l'extension du nom de domaine en question, du droit antérieur invoqué et du contexte de la situation, différentes options sont ouvertes : la procédure Syrelli pour les noms de domaine en .fr, la plainte UDRP pour les noms de domaine génériques de premier niveau (gTLDs) et correspondant aux codes de pays (ccTLDs) ou encore la plainte URS pour les nouvelles extensions.

Le choix de la procédure n'est pas anodin puisqu'elle est fonction de la situation et nécessite une étude juridique en amont pour déterminer la meilleure option selon l'exploitation du nom de domaine, les droits antérieurs, les conditions requises et l'objectif recherché. Et pour pouvoir détecter en amont ces « cybersquattings », nous rappelons l'importance de mettre en place une surveillance de sa marque parmi les noms de domaine afin de réagir rapidement et efficacement.

- Un monitoring web : indispensable pour garantir au consommateur l'origine des produits ou services proposés par la marque, une surveillance sur internet doit être mise en place afin de pouvoir identifier le contenu et l'évolution de site web reproduisant la marque (dénomination, logo ou slogan) en question. Cette surveillance peut porter sur les différents canaux de communication : applications mobiles, réseaux sociaux (Facebook, Instagram, Twitter, LinkedIn, YouTube, WeChat…), sites marchands (eBay, Amazon, Alibaba, AliExpress, Tmall.com, Taobao et IndiaMART…), contenu de site web et noms de domaine (extensions territoriales, génériques ou nouvelles extensions). Elle permet de détecter rapidement une utilisation non autorisée du signe identitaire, d'analyser le trouble qui y est porté et enfin d'agir promptement afin de faire cesser l'atteinte.

La sécurisation de l'usage des marques sur internet est devenue l'un des défis majeurs actuels pour les titulaires de droits afin de protéger le consommateur contre les contrefaçons et garantir l'origine des produits et services.

Colombe Dougnac
Conseil en Propriété Industrielle – Marques, Dessins et Modèles, Novagraaf, France. Pour la contacter : brandprotection@novagraaf.com.

Focus sur ces cinq modules

D'après notre expérience, les cinq canaux de diffusion suivants sont les plus importants en matière de contrôle et de mise en œuvre d'actions :

- **Applications** : Si les applications peuvent aider les marques à accroître et à améliorer les interactions avec leurs consommateurs et à recueillir des informations sur le marché, elles constituent un autre domaine de fraude potentielle des marques. Surveillez les applications et les éditeurs d'applications qui mentionnent une marque dans le nom de l'application ou dans le nom de l'éditeur, afin de fournir aux marques les informations dont elles ont besoin pour évaluer et prendre des mesures.
- **Noms de domaine** : Le cybersquatting est un problème permanent pour les propriétaires de marques. L'approche la plus efficace consiste ici à choisir un service de surveillance des noms de domaine qui identifie automatiquement l'utilisation non autorisée d'un nom de marque dans les noms de domaine nouvellement enregistrés, et propose ou automatise les mesures appropriées, de la simple surveillance de la menace potentielle aux mesures de démantèlement et aux principes UDRP.
- **Site marchands** : Il est important de surveiller les infractions potentielles sur les principales plateformes de e-commerce, telles que eBay, Amazon, Alibaba, AliExpress, Tmall.com, Taobao et IndiaMART. Le dépistage fournira des informations précieuses sur la manière dont les biens et services de marque sont vendus sur ce marché en ligne et fournira les outils nécessaires pour éliminer ces menaces.
- **Réseaux sociaux** : Malheureusement, les médias sociaux sont un canal de plus en plus populaire pour la contrefaçon et d'autres formes d'infraction. Toutes les grandes plateformes de médias sociaux doivent être surveillées, y compris Facebook, Instagram, Twitter, LinkedIn, YouTube, WeChat (Chine), Weibo (Chine) et VKontakte (Russie), en identifiant également les modèles et les récidivistes en vérifiant le nom du compte et le traffic.
- **Contenus web** : Surveillez les violations potentielles dans le contenu en ligne des sites web indexés par les principaux moteurs de recherche, que la marque apparaisse ou non dans le nom de domaine, par exemple les sites à apparence similaire. Il s'agit notamment d'identifier les menaces pesant sur une marque sur les sites web apparaissant dans les résultats des principaux moteurs de recherche, dans les liens, le contenu des pages, les images (en utilisant les technologies de reconnaissance d'images) et les métabalises.

Selon votre entreprise, certains ou potentiellement tous ces canaux devront être surveillés, et plus vos activités de surveillance et d'application seront synchronisées, plus elles seront susceptibles d'être efficaces et performantes. Découvrez comment ce service novateur peut vous aider à cet égard en demandant une démonstration de notre service de protection des marques en ligne à l'adresse suivante : **novagraaf.com/fr/brand-protection**.

Etendre son territoire de marque sur le web

Chaque jour, près de 30 millions de contenus sont partagés sur les espaces digitaux par les entreprises, les journalistes, les artistes, les institutions, les politiciens, sans oublier bien sûr les particuliers.

Vidéos, photos, petits textes, blogs, sites informatifs, petites annonces, on trouve de tout sur le web, mais ce qu'il est souvent difficile de trouver, c'est l'auteur de ces contenus.

Le web permet de se dissimuler derrières des pseudonymes et des avatars et l'anonymat devient la règle, en particulier depuis l'application extensive des dispositions du Règlement Général sur la Protection des Données (RGPD) dictée par l'ICANN.

Il est facile dans ces conditions, de se laisser aller à toutes sortes de dérives et notamment les contrefaçons qui nous intéressent particulièrement dans ce livre blanc.

Les contrefaçons sur le web peuvent prendre de nombreuses formes qui ont des conséquences très différentes les unes des autres comme on a pu le voir plus haut.

Or, les clients exigent de plus en plus des marques qu'elles exercent leur rôle de garantie d'origine.
Les marques peuvent avoir un rôle actif pour protéger leur espace mais également créer un réflexe de contrôle chez les internautes.

Un moyen d'être proactif plutôt que réactif, face aux évolutions des comportements d'achat et à la création incessante de canaux de communication et de distribution.

Outre la surveillance et la répression à mettre en place, l'ICANN a ouvert depuis 2012 une nouvelle solution très efficace pour les marques : le .marque.

Ouverture à l'enregistrement de nouveaux TLD

Avant toute chose, rappelons de quoi se compose une adresse web (URL) : **https://www.novagraaf.com**

https:// indique au navigateur le protocole qui doit être utilisé pour récupérer le contenu, c'est-à-dire le langage utilisé pour communiquer sur le réseau. Le protocole le plus utilisé est HTTP ou sa version sécurisée : HTTPS.

www. : sous-domaine. Il s'agit de la norme pour aller sur un site web, sur le world wide web. Cette partie n'est pas obligatoire dans une adresse URL

novagraaf.com : le nom de domaine. Il indique le serveur web auquel le navigateur s'adresse pour échanger le contenu. Il s'agit souvent de la marque ou du nom de la société.

Au sein de ce nom de domaine, on distingue le domaine de 1e niveau, Top Level Domain (TLD), ou extension (ici, le .com), et le domaine de second niveau (ici, novagraaf), placé avant le point.

On peut ajouter des sous-domaines, soit chaque dénomination placée avant chaque point :
france.novagraaf.com / newsletter.novagraaf.com etc.

En 2008, face à la pénurie de noms de domaine courts disponibles dans les extensions génériques (gTLD) ou nationales (ccTLD pour country code Top Level Domain), l'ICANN a ouvert au public la possibilité de créer et gérer de nouveaux TLD.

Ce programme a permis à toute personne de déposer, début 2012, un dossier de demander pour devenir registre de sa propre extension.

On a isolé 4 catégories de TLD :

- **Extensions communautaires** : renvoyant à une communauté culturelle, cultuelle, sportive etc : .catholic, .tennis, .gay etc
- **Extensions géographiques** : qui agissent comme une garantie d'origine, pour certaines zones géographiques, comme un gage d'une certaine qualité.: .paris, .alsace, .bzh
- **Extensions génériques** : catégorie fourre-tout, renvoyant généralement à une catégorie de produits/services : .wine, .pizza, .bio, .porn
  Tout est dans le titre, on sait ce que l'on y trouvera.
- **Extensions de marques** : permettant aux sociétés d'utiliser leur propre marque ou tout autre terme affilié, comme extension.

Chacun pouvait ainsi déposer un dossier de demande de nouveau TLD générique, choisi tout à fait librement.

L'ICANN a lancé ce projet totalement novateur sans trop savoir à quoi s'attendre et a ainsi reçu près de 2.000 demandes de nouveaux noms de domaine génériques et 1248 nouvelles extensions génériques ont été créées depuis 2012.

BrandTLD : une solution efficace à un problème tenace

Le .marque, qui nous intéresse particulièrement, permet de se construire une identité numérique distinctive en capitalisant sur ce qui définit la société : sa marque.

Il offre un territoire totalement maîtrisé et sécurisé sur le web.

609 .marque ont ainsi été créés en 2012, dont 491 bénéficiant de la spécification 13, permettant au registre de conserver une utilisation exclusive de leur extension.

Le brandTLD est un registre fermé dont vous avez le total contrôle. Il ne peut donc pas y avoir d'abus sur cet environnement.

Tous les noms de domaine dont vous avez besoin sont disponibles sous cette extension. La seule limite est votre imagination et l'indisponibilité de la dénomination que vous briguez, en .com ou .fr, ne sera plus un obstacle.

En outre, l'acquistion du .marque est l'occasion de repenser votre environnement numérique pour plus de clarté et de sécurité. Vous pouvez mettre en avant un produit, un franchisé, une activité.

Les exemples les plus marquants en France sont évidemment BNP PARIBAS et la SCNF avec oui.sncf, qui ont totalement refondu leur site et revu leur communication pour intégrer cette nouveauté et en faire un atout.

C'est globalement dans le domaine bancaire qu'on a trouvé le plus d'engouement face au .marque. Cela peut s'expliquer tout d'abord par la multitude de services proposés et la nécessité de simplicité pour les clients, mais également par le besoin poussé des banquesd'assurer une sécurité totale de leurs espaces digitaux. Le .marque dans ce secteur permet de garantir à l'internaute qu'il est sur le bon espace et que les données qu'il entre sont bien destinées à sa banque et à nul autre.

En France, **BNP Paribas** a par exemple créé un site en .bnpparibas, par type d'activité :

- banque avec https://mabanque.bnpparibas/
  Lui-même réparti par public :
  - banque privée : https://mabanqueprivee.bnpparibas/
  - banque d'entreprises : https://banqueentreprise.bnpparibas/
  - Et bien sûr le site institutionnel https://group.bnpparibas/en/

Etonnamment pourtant, très peu de propriétaires de brandTLD ont migré totalement leur site sur leur .marque.

En effet, la plupart des entreprises ayant pourtant largement investi pour obtenir leur .marque, sont plus frileux et utilisent leur extension pour des mini sites consacrés à la promotion d'un produit ou d'un service.

Ainsi, **Total** a mis à l'honneur sa fondation sur le .total, avec le site dédié https://www.foundation.total/fr/accueil.

Le groupe E. Leclerc a également largement communiqué sur le .leclerc, mais n'a lui aussi utilisé son extension que pour des mini sites dédiés à une activité particulière :
- culture : https://www.culture.leclerc/
- hightech : https://www.hightech.leclerc/cart

Audi a misé sur :
- un réseau web pour les professionnels : kundendialog.audi
- un réseau de pièces détachées pour tous les garages du monde : gebrauchtteile.audi
- la mise en avant de produits pour les clients :
  - e-tron.audi
  - aime.audi

En revanche, il s'agit pour la plupart de ces sites de redirections (parfois d'ailleurs vers une autre nouvelle extension générique, comme le .vision).

Plusieurs sociétés ont pris ce parti d'un usage très restreint.

Microsoft, pourtant très au point sur les questions web et le renforcement de sa position sur le web, se contente également, pour le moment de rediriger sur le .com, en attendant que les internautes ne prennent l'habitude de taper une URL en .marque .

D'autres enfin n'utilisent pas du tout leur .marque, malgré les sommes engagées.

Les possibilités sont pourtant énormes autour de l'extension marque, pour assurer un environnement dédié totalement sécurisé et une communication claire.

Le .marque devient également un outil marketing puissant. Les premières sociétés à avoir investi et communiqué sur le .marque passent pour des entreprises innovantes, et avec la bonne communication (comme pour oui.sncf par exemple), les avantages en termes de communication sont très importants.

Enfin, d'un point de vue sécurité, le .marque assure à une société le contrôle total de tous les noms de domaine enregistrés sous son extension et permet de se prémunir de tout enregistrement frauduleux.

Bien éduqué avec une communication intensive et appropriée, l'internaute qui navigue sur les sites du .marque sait qu'il est sur un environnement sûr et est garanti contre toute tentative de phishing, ou achat de contrefaçon.

Le .marque agit en effet comme le .gouv.fr en France ou le .gov.uk par exemple, qui garantissent à l'internaute qu'il est sur un site institutionnel et trouvera les informations officielles. Il a en revanche l'avantage d'éviter les adresses URL à rallonge.

Sans oublier que l'extension .marque est un actif incorporel immobilisé et participe à la valeur de l'entreprise.

En effet, les BrandTLDs sont assimilés à des noms de domaine, c'est-à-dire des signes distinctifs pouvant être attachés au régime juridique général des marques.

Prochain round attendu

L'ICANN va ouvrir un prochain round de TLD.

Néanmoins, les discussions ont pris beaucoup de retard et ce round n'est pas attendu avant 2022/2023, ce qui laisse le temps aux entreprises de prendre leur décision et anticiper les démarches ;

Un dossier de candidature doit être déposé à l'ICANN dans un calendrier qui sera fourni en temps utiles. La préparation de ce dossier prend au minimum 6 mois et doit comporter de nombreuses informations quant à la composition de l'entreprise, son business plan, la sécurité technique, la protection de la marque etc.

Il convient également de ne pas négliger les réflexions sur la communication digitale. Que ferez-vous de votre brandTLD ?

Une fois l'ouverture décrétée, chaque candidat devrait avoir un créneau de six mois pour déposer son dossier.

L'étude de ce dossier prend ensuite entre 6 et 12 mois. Des discussions sont en cours pour accorder un fast-track pour les .marque, en particulier bénéficiant de la spécification 13, puisque les risques de sécurité sont nécessairement moins importants pour les extensions évoluant ainsi en circuit fermé.

En 2012, chaque candidat devait verser, avec son dossier, une somme de 185.000$.

Le tarif du prochain round n'est pas encore connu mais il n'est pas garanti que l'ICANN baisse ses prétentions, malgré le trésor inattendu amassé en 2012.

Mais ce n'est pas tout, puisque la gestion technique annuelle de l'extension a également un coût, autour de 25.000$ par an.

En parallèle, vous économisez l'enregistrement de noms de domaine, vous pouvez également gagner de l'argent dans les modèles de franchise par exemple, où vous permettriez aux franchisés l'enregistrement d'un nom de domaine dans votre extension, moyennant un coût d'enregistrement annuel.

Vous économiserez également, à terme, en frais de protection juridique sur le web car avec une bonne communication, les atteintes ne prendront plus sur vos clients, habitués à naviguer uniquement sur le .marque.

L'acquisition d'un BrandTLD peut s'avérer un réel atout pour une société et il est tout à fait pertinent d'en discuter en interne mais également avec vos Conseils en Propriété Intellectuelle et prestataires techniques.

Laurence Rivière
Conseil en Propriété Industrielle – Marques, Dessins et Modèles, Novagraaf, France. Pour la contacter : brandprotection@novagraaf.com.

Novagraaf
A NovumIP Company

La protection de marques en ligne de Novagraaf

Une solution moderne qui répond à un problème actuel

En tant que juristes spécialisés garant de la stratégie de Propriété iIntellectuelle de nos clients et de sa mise en œuvre, nous disposons des connaissances, de l'expérience et de la portée mondiale nécessaires pour intégrer de manière transparente la protection de marques en ligne dans la stratégie de Propriété Intellectuelle de votre entreprise. Conscients des contraintes de temps et de ressources qui pèsent sur les services internes de Propriété Intellectuelle et de protection des marques, ainsi que sur les cabinets de PI. C'est pourquoi nous avons mis au point un service sur-mesure et entièrement accessible en ligne qui vous informera des résultats pertinents, vous proposera des solutions pratiques en accord avec votre stratégie de Propriété Intellectuelle au sens large et luttera efficacement contre les menaces qui pèsent sur la présence de votre marque en ligne. Notre protection de marques en ligne permet d'avoir une vue d'ensemble des risques en ligne, facilite les mesures d'application et détecte les schémas de menace afin de mieux suivre les infractions et de prendre des mesures à leur encontre.

- Les mesures d'exécution sont prédéfinies, ce qui réduit les exigences imposées à vos équipes internes ;
- Les actions plus courantes sont automatisées via le CMS, de sorte que leurs mises en oeuvre soient plus rapides et rentables ;
- L'activité est ciblée par type de menace ;
- Les effets de la surveillance et de la mise en œuvre des actions sont disponibles via un portail unique, combinant l'expertise d'analystes et de juristes ;
- Le service est soutenu par le réseau mondial de juristes en Propriété Intellectuelle de Novagraaf, ce qui permet de prendre rapidement et stratégiquement des mesures d'exécution supplémentaires, indépendamment de la géolocalisation.

Le service comprend un rapport panoramique des menaces en ligne afin de générer une étude préliminaire sur l'aspect général de votre marque en ligne. Ce rapport est utilisé pour déterminer les paramètres des phases de surveillance et de mise en oeuvre de la loi afin de répondre au mieux à vos objectifs et de prédéfinir les actions nécessaires, le budget (par marque/module) et les éléments déclencheurs de toute activité stratégique supplémentaire.

Pour en savoir plus, consultez le site **novagraaf.com/fr/brand-protection** ou contactez-nous à l'adresse **brandprotection@novagraaf.com**.